

AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

FILED

AUG - 3 2018

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

Item listed in Attachment A. Located at Google, Inc., a company headquartered
at 1600 Amphitheatre Parkway in Mountain View, California 94043.

Case No. 4:18 MJ 6280 PLC

APPLICATION FOR A SEARCH WARRANT

I, David Herr, a federal law enforcement officer or an attorney for the government
request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 USC § 1201, 2422, 2423(a)

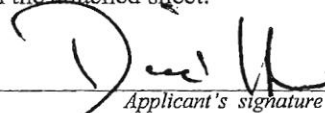
Offense Description

Kidnapping, Coercion and Enticement, Transportation of a Minor

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

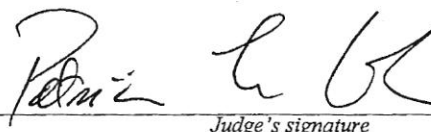


Applicant's signature

David Herr, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 8-3-18


Judge's signature

City and state: St. Louis, MO

Honorable Patricia L. Cohen, U.S. Magistrate Judge

Printed name and title

AUSA: Colleen L. Lang

FILED
AUG - 3 2018
U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, David Herr, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under Title 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Inc., to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications, related to the accounts associated with the email addresses of "[REDACTED]@gmail.com" and "[REDACTED]@gmail.com". The information to be seized is described in the following paragraphs and in Attachment B.

2. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

3. This affidavit is made in support of an application for a search warrant to search for and seize instrumentalities, fruits, and evidence of violations of Title 18, U.S.C. Section 1201, Kidnapping, Title 18, U.S.C. Section 2423(a), Transportation of Minors, and Title 18, U.S.C.

Section 2442, Coercion and Enticement. The items that are the subject of the search and seizure applied for in this affidavit are more specifically described in Attachments A and B.

4. I make this affidavit in support of an application for a search warrant for any and all information related to kidnapping, transportation of a minor across state lines, and using the mail or any facility or means of interstate or foreign commerce to knowingly persuade, induce, entice or coerce a person under the age of 18 to engage in sexual activity: as may be found associated with certain accounts that are stored at the premises owned, maintained, controlled, and/or operated by Google, Inc., a company and email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described below and in Attachment A, attached hereto. This affidavit is made in support of an application for a search warrant under Title 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the “angelderhardt669@gmail.com” and “angelderhardt24@gmail.com” email accounts, including the contents of communications. I prepared this affidavit in support of an application for a search warrant because I believe the subject email addresses/accounts contain evidence of violations of Title 18, U.S.C. Section 1201, Kidnapping, Title 18, U.S.C. Section 2423(a) Transportation of Minors, and Title 18, U.S.C. Section 2442, Coercion and Enticement.

5. The statements contained in this affidavit are based on this affiant’s personal knowledge or information provided to this affiant by other law enforcement officers and other agencies. Since this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to me concerning this investigation. This affiant has set forth only the facts that I believe are necessary to establish probable cause to believe that

evidence, fruits, and instrumentalities of violations of Title 18, U.S.C. Section 1201, Kidnapping, Title 18, U.S.C. Section 2423(a) Transportation of Minors Title 18, U.S.C. Section 2442, Coercion and Enticement, including but not limited to the items described on Attachment B, which is attached hereto and incorporated herein by reference, will be found within the following Google G-mail accounts of A [REDACTED] B [REDACTED]:

- a. [REDACTED]@gmail.com
- b. [REDACTED]@gmail.com

LOCATIONS TO BE SEARCHED

Pursuant to Title 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) your affiant is asking the court to direct Google, Inc., to disclose to the government any and all information in its possession pertaining to the subscriber or customer associated with the following Subject Email Addresses/Accounts: "angelderhardt669@gmail.com" and "angelderhardt24@gmail.com" which are maintained by Google, Inc. through its computer systems. These locations are more fully described in Attachment A, attached hereto.

Statutory Authority

This investigation concerns alleged violations of Title 18, United States Code, Section 2252A, relating to the sexual exploitation of minor Title 18, U.S.C. Section 1201, Kidnapping, Title 18, U.S.C. Section 2423(a) Transportation of Minors, Title 18, U.S.C. Section 2422, Coercion and Enticement. Title 18, U.S.C. Section 1201, the federal kidnapping statute, prohibits a person from knowingly seizing or confining a person and holds for ransom or reward. Title 18 U.S.C. Section 2423(a) criminalizes transporting a minor across state lines with the intent to engage in sexual activity. Title 18, U.S.C. Section 2422 criminalizes knowingly persuading, induced,

enticing or coercing a minor to engage in any sexual activity for which a person can be charged with a criminal offense.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711 and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

DEFINITIONS

8. The following definitions apply to this Affidavit and the Attachments to this Affidavit:

a. Visual depictions include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image.

See 18 U.S.C. § 2256(5).

b. Sexually explicit conduct means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

c. The term "computer," as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as an "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

d. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

f. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form

(including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

h. "Computer passwords" and "data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might be static whereby the user's ISP assigns his computer a unique IP address – and that same number is used by the user every time his computer accesses the Internet. Numerical IP addresses generally have corresponding domain names. For instance, the IP address 149.101.10.40 traces to the corresponding domain name

"www.cybercrime.gov". The Domain Name System or DNS is an Internet service that maps domain names. This mapping function is performed by DNS servers located throughout the Internet. In general, a registered domain name should resolve to a numerical IP address.

j. "Internet addresses" take on several forms, including Internet Protocol (IP) addresses, Uniform Resource Locator (URL) addresses, and domain names. Internet addresses are unique and can be traced to an identifiable physical location and a computer connection. The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.187). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address, it enables Internet sites to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs. There are two types of IP addresses, dynamic and static. To assign dynamic IP addresses, the ISP randomly assigns one of the available IP addresses, in the range of IP addresses controlled by the ISP, each time a customer dials in or connects to the ISP in order to connect to the Internet. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, that IP address becomes available to other customers who dial in at a later time. Thus, an individual customer's dynamic IP address may, and almost always will, differ each time he dials into or connects to the ISP. To assign static

IP addresses, the ISP assigns the customer a permanent IP address. The customer's computer would then be configured with this IP address every time he dials in or connects to the ISP in order to connect to the Internet.

k. The "Internet" is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of sharing information. Connections between Internet computers exist across state and international borders and information sent between computers connected to the Internet frequently crosses state and international borders, even if those computers are in the same state. A network is a series of devices, including computers and telecommunication devices, connected by communication channels.

l. An "internet service provider" (ISP) is a commercial service that provides Internet connectivity to its subscribers. In addition to providing access to the Internet via telephone lines or other telecommunications lines, ISPs may also provide Internet e-mail accounts and other services unique to each particular ISP such as Usenet Newsgroups and Internet Relay Chat. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, customer service information and other information, both in computer data format and in written record format.

m. A "server" is a centralized computer that provides services for other computers connected to it via a network. The computers that use the server's services are sometimes called "clients."

n. A Minor means any person under the age of eighteen years (18 U.S.C. ' 2256(1)).

Background information regarding Computers, the Internet and E-mail:

- a. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.
- b. Computers connected to the Internet are identified by addresses. Internet addresses take on several forms, including Internet Protocol (IP) addresses, Uniform Resource Locator (URL) addresses, and domain names. Internet addresses are unique and can identify a physical location and a computer connection.
- c. Electronic mail (or "e-mail") is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends e-mail, it is initiated at the user's computer, transmitted to the subscriber's mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means.

Background of Google, Inc. and GMAIL

Based on my experience and training, as well as information from public records, your Affiant knows the following:

- a. Google, Inc., which is physically headquartered at 1600 Amphitheatre Parkway in Mountain View, California 94043, provides free web-based Internet electronic mail ("e-mail") to the general public, and that stored electronic communications, including

opened and unopened e-mail for Gmail subscribers may be located on Google, Inc.'s computer system.

b. I have learned Google, Inc. ("Google"), provides a variety of on-line services, including electronic mail ("E-mail") access, to the general public. Google allows subscribers to obtain E-mail accounts at the domain name (*i.e.*, gmail.com), like the E-mail accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved E-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, E-mail transaction information, and account application information.

c. In general, an E-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the E-mail. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the E-mail, it may continue to be available on Google's servers for a certain period of time.

d. When the subscriber sends an E-mail, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google often saves a copy of the E-mail sent. Unless the sender of the E-mail specifically deletes the E-mail from the Google server, the E-mail can remain on the system indefinitely. Even if the sender deletes the E-mail, it may continue to be available on Google's servers for a certain period of time.

e. A sent or received E-mail typically includes the content of the message, source and destination addresses, the date and time at which the E-mail was sent, and the size and length of the E-mail. If an E-mail user writes a draft message but does not send it, that message may also be saved by Google, but may not include all of these categories of data.

f. A Google subscriber can also store files, including E-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Google. Subscribers to Google might not store on their home computers copies of the E-mails stored in their Google account. This is particularly true when they access their Google account through the web, or if they do not wish to maintain particular E-mails or files in their residence.

g. In general, E-mail providers like Google ask each of their subscribers to provide certain personal identifying information when registering for an E-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative E-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

h. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website), and other log files that reflect usage of the account. In addition, E-mail providers often have records of the Internet

Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the E-mail account.

i. In some cases, E-mail account users will communicate directly with an E-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

j. In my training and experience, evidence of who was using an E-mail account may be found in address books, contact or buddy lists, E-mail in the account, and attachments to E-mails, including pictures and files.

k. Computers located at Google, Inc. contain information and other stored electronic communications belonging to hundreds of thousands of third parties unrelated to this investigation. Accordingly, this Affidavit and Application for Search Warrant seek authorization solely to search the computer accounts and/or files set forth in Attachment

A.

Stored Wire and Electronic Communication Access

9. Title 18, United States Code, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications and Transactional Records Access."

a. Title 18, United States Code, Section 2703(a) provides, in part:

A governmental entity may require the disclosure by a provider of electronic communication service the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure by a Court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

b. Title 18, United States Code, Section 2703(b) provides, in part:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –

(A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the procedures described in the the Federal Rules of Criminal Procedure by a Court with jurisdiction over the offense under investigation or equivalent State warrant...

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service: –

(A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission

from), a subscriber or customer of such remote computing service;
and

(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

c. The government may also obtain records and other information pertaining to a subscriber or customer of electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c). No notice to the subscriber or customer is required. 18 U.S.C. § 2703(c)(2).

d. Title 18, United States Code, Section 2711, provides, in part:

As used in this chapter –

(1) The terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) The term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

e. Title 18, United States Code, Section 2510, provides, in part:

(A) "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; . . .

(B) "Electronic communications system" means any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications and any computer facilities or related electronic equipment for the electronic storage of such communications; . . .

(C) "Electronic communication service" means any service, which provides to users thereof the ability to send or receive wire or electronic communications; . . .

"Electronic storage" means --

- (1) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
- (2) Any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

Investigation

10. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since August 1998. As such, I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516(1). My current assignment is the St. Louis Division, where I investigate violent crimes, to include carjacking, kidnappings, Hobbs Act robberies, and persons prohibited from possessing firearms. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

11. The statements in this affidavit are based in part on this affiant's personal knowledge or information provided by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to her concerning this investigation.

12. On July 22, 2018, the Jefferson County Sheriff's Office was contacted by Tanya Hall, the mother of A [REDACTED] E [REDACTED], who is her legal custodian. E [REDACTED] is a 15-year-old juvenile. Hall stated that at approximately 8:30 A.M. on July 22, 2018, she went to E [REDACTED]'s bedroom and discovered E [REDACTED] was missing. The bedroom window was open and the screen had been removed. On E [REDACTED]'s bed, Hall discovered a pile of clothing under the blanket, mimicking a human body.

13. Also noted on the bed was a tape recorder with a note stating, "Play me". The tape recording, which only contained E [REDACTED]'s voice stating that she was going off to Germany. E [REDACTED] stated she did not want her family to report her as missing. Below is a partial transcription of the audio recording:

"Don't put me on Facebook as missing. Don't put me on the news or anything. I'll be watching. I know that's going to be really hard for you. But, you can't put me out there. If you do, then I'm gonna commit suicide because I don't want people looking for me. As long as you don't tell everyone, you don't call the cops or anything, I'll be okay and I'll be safe. Later in the recording, E [REDACTED] stated, "Um, I'll be back when I'm 18."

14. On August 1, 2018, Hall was re-interviewed by Law Enforcement. Hall stated that E [REDACTED] had no credit / debit cards, and no passport. Hall stated E [REDACTED] may have \$5 at the most. Hall also stated that E [REDACTED] had no history of being a runaway and there was no recent turmoil in the

family that would have indicated that E█████ would run away. Hall stated that she noticed several items belonged to E█████ were missing. Those items included her cell phone, a large plastic bag containing newly purchased clothing for the upcoming school year, and blue denim jacket. Furthermore, Hall stated that one or two days prior to E█████ disappearing, Hall caught E█████ taking what she believed to be sexually explicit photographs. Specifically, Hall stated she entered E█████'s room and saw E█████ pulling down her shirt while holding her phone. It appeared to Hall that E█████ has just taken a picture of her bare chest with the cell phone. When confronted about what E█████ was doing, she simply said she was changing clothing. I know from discussing this with agents, who have training and experience in child sexual exploitation cases, that this behavior is consistent with the grooming process of victims in online enticement of minor cases. Hall again stated that E█████ had no access to money, no credit card, no passport, and "May have \$5." E█████ did not have a history being a runaway and there were no recent domestic incidents that would cause E█████ to run away. Hall had also been monitoring E█████'s social media presence, which according to Hall, E█████ used on a very frequent basis. Since July 22, 2018, Hall has seen no presence of E█████ on social media. Hall has also attempted to call E█████'s phone, but calls have gone straight to voice mail since July 22, 2018. As of E█████ has had her own iPhone 6 cell phone since approximately November of 2017. The iPhone is web-enabled smart phone that allows the user to access the internet and their social media applications.

15. On August 2, 2018, Law Enforcement interviewed a neighbor of E█████. The neighbor stated that sometime between 2 and 3 A.M. on July 22, 2018, they observed a smaller mid-sized Sports Utility Vehicle, similar to a Ford Explorer, parked on White Road near Woods Road, in Hillsboro, Missouri, facing the direction of E█████'s residence. The neighbor stated that vehicle had an out of state license plate, possibly yellow in color. The neighbor noticed a female wearing

a blue coat carrying a large shopping bag walking from the direction of E [REDACTED]'s residence on White Road toward the vehicle. That description of the coat and bag is consistent with the items that Hall reported to be missing from E [REDACTED]'s residence. Investigators reviewed satellite images of the area and there appeared to be no other residences in the area of the above-described path between E [REDACTED]'s residence and the location where the vehicle was parked.

16. On July 30, 2018, law enforcement officers contacted AT&T and AT&T responded that on July 30, 2018 at 04:51:21 A.M. Universal Time Coordinated, July 29, 2018, 11:56:21 Central Standard Time, the target phone (636) 208-2238, was noted by AT&T to have had a NELOS ("Network Event Location System") hit. The hit showed that at that time on July 29, 2018, the phone had GPS coordinates of Latitude 38.566296, Longitude -90.033894. Those coordinates resolved back to a cellular tower located in Belleville, Illinois, indicating that the phone was physically proximate to Belleville, Illinois.

17. This affiant knows from training and experience, as well as, from information received from other law enforcement officers, that minors meet adults online. Based on my training and experience, adults who are interested in communicating with minors online via social media applications, often do so because they are interested in a sexual activity with minors. Adults who meet minors online often try and coerce the minors to meet them to engage in sexual activity.

18. This affiant knows from training and experience that children communicating with persons interested in the kidnapping and/or transportation or enticement of a minor to engage in any sexual contact can communicate with those children through email accounts like Gmail. Further, this affiant knows that the missing minor, A [REDACTED] B [REDACTED], had two Gmail email accounts. These email accounts have the following email addresses: "[REDACTED]@gmail.com" and "[REDACTED]@gmail.com"

Gmail stores communications and emails, as well as, IP address information associated with the email communications within its accounts on Google Inc.'s computer servers. I believe this information in the email accounts could lead us to identify whom the missing minor child is with, whom she has been communicating with, and possibly her location.

19. This affiant knows from training and experience that children communicating with persons interested in the kidnapping, transportation of minor, and/or enticement of a minor to engage in any sexual contact often communicate with those children through online through email and social media accounts. This correspondence could provide identifying information regarding either the child or those persons she with, to include, but not limited to, his/her names, addresses, online account usernames, phone numbers, Internet Protocol (IP) addresses, GPS coordinates, logged dates and times of communications, the content of message exchanges, and identifying photographs and/or videos.



20. This affiant know from training and experience that even if digital information is deleted by the user, the deleted information may still be accessible by the social media and/or online account provider.

21. Your affiant respectfully requests that the affidavit and search warrant be sealed so as not to compromise this on-going investigation.

Search Procedure

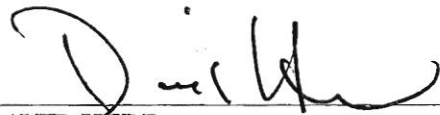
22. In order to ensure that agents search only those computer accounts and/or files described in Attachment A, this affidavit and application for search warrant seek authorization to permit employees of Google, Inc., to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those computer accounts and/or files described in Attachment A the following procedures will be implemented:

- a) The search warrant will be presented to Google, Inc., personnel who will be directed to isolate those accounts and files described in Attachment A;
- b) In order to minimize any disruption of computer service to innocent third parties, Google, Inc., employees and law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Attachment A, including an exact duplicate of all information stored in the computer accounts and files described in Attachment A;
- c) Google, Inc., employees will provide in electronic form the exact duplicate of the accounts and files described in Attachment A and all information stored in those accounts and files to the agent who serves this search warrant;
- d) Law enforcement personnel will thereafter review the information stored in the accounts and files received from Google, Inc., employees and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant; and,
- e) Law enforcement personnel will then seal the original duplicate of the accounts and files received from Google, Inc., employees and will not further review the original duplicate absent an order of the Court.

23. Based upon the aforementioned information, your affiant believes that probable cause exists that the Google, Inc., accounts having the email addresses of “@gmail.com” and “@gmail.com” and which are stored at the premises owned, maintained, controlled, or operated by Google, Inc., located at 1600 Amphitheatre Parkway in Mountain View, California 94043, has evidence as listed in

Attachment B and relating to the kidnapping and/or transportation/enticement of a minor to engage in any sexual act or sexual contact.

24. Specifically, it is believed Google, Inc., has records regarding these accounts' various communications, messages, snaps, stories, chats, memories, images, videos, electronic storage, "follower" and/or "friend" lists, subscriber information, terms of service violation reports, detailed billing records, and/or any and all other content, which contain evidence of violations of Title 18, U.S.C. Section 1201, Kidnapping, Title 18 U.S.C. Section 2423(a) Transportation of a Minor Across State lines and Title 18, U.S.C. Section 2422, Coercion and Enticement, as described in Attachment B.



DAVID HERR
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me this _____ day of August, 2018.

PATRICIA L. COHEN
United States Magistrate Judge
Eastern District of Missouri

ATTACHMENT A

Property to Be Searched

All records regarding the Google, Inc., accounts with the usernames of

“[REDACTED]@gmail.com” and “[REDACTED]@gmail.com”, and any and all other

information maintained by Google, Inc., a company headquartered at 1600 Amphitheatre

Parkway in Mountain View, California 94043, for the period of October 1, 2017 to the date this

warrant is received.

ATTACHMENT B

Particular Things to be Seized

- a. Any and all correspondence and/or content, to include but not limited to communications, messages, chats, emails, attachments, images, videos, electronic storage, “follower” and/or “friend” lists, subscriber information, terms of service violation reports, detailed billing records, which pertains to the enticement of a minor to engage in any sexual act or sexual contact;
- b. Any and all correspondence and/or content, to include but not limited to communications, messages, chats, emails, attachments, images, videos, electronic storage, “follower” and/or “friend” lists, subscriber information, terms of service violation reports, detailed billing records, which pertains to the kidnapping of a child.
- c. Any and all correspondence and/or content, to include but not limited to communications, messages, chats, emails, attachments, images, videos, electronic storage, “follower” and/or “friend” lists, subscriber information, terms of service violation reports, detailed billing records, which appears to contain passwords or information regarding encryption;
- d. Any and all transactional information, to include log files (transmission and usage) of all activity of the accounts, to include dates, times, methods of connecting, ports, dial-ups, locations, originating Internet Protocol (IP) addresses and/or destination IP addresses for any and all correspondence and/or content, to include but not limited to communications, messages, chats, emails, attachments, images, videos, electronic storage, “follower” and/or “friend” lists, subscriber information, terms of service violation reports, detailed billing records;
- e. All GPS or location information stored by Google, Inc. in relation to these accounts;
- f. Any records of subscriber information, methods of payment, or detailed billing; and,

g. Copies of all the above from original storage on whatever form, to include printouts

and/or digital format.

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

FILED

AUG - 3 2018

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

Item listed in Attachment A. Located at Google, Inc., a company
headquartered at 1600 Amphitheatre Parkway in Mountain View, California
94043.

Case No. 4:18 MJ 6280 PLC

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the NORTHERN District of CALIFORNIA
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENT B

YOU ARE COMMANDED to execute this warrant on or before August 17, 2018 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

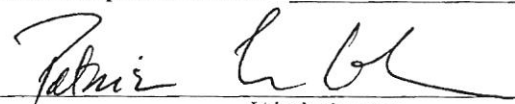
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to United States Magistrate Judge Patricia L. Cohen
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued: 8-3-18 1:55 P.M.


Judge's signature

City and state: St. Louis, MO

Honorable Patricia L. Cohen, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

All records regarding the Google, Inc., accounts with the usernames of

"[REDACTED]" and "[REDACTED]", and any and all other

information maintained by Google, Inc., a company headquartered at 1600 Amphitheatre

Parkway in Mountain View, California 94043, for the period of October 1, 2017 to the date this

warrant is received.

ATTACHMENT B

Particular Things to be Seized

- a. Any and all correspondence and/or content, to include but not limited to communications, messages, chats, emails, attachments, images, videos, electronic storage, “follower” and/or “friend” lists, subscriber information, terms of service violation reports, detailed billing records, which pertains to the enticement of a minor to engage in any sexual act or sexual contact;
- b. Any and all correspondence and/or content, to include but not limited to communications, messages, chats, emails, attachments, images, videos, electronic storage, “follower” and/or “friend” lists, subscriber information, terms of service violation reports, detailed billing records, which pertains to the kidnapping of a child.
- c. Any and all correspondence and/or content, to include but not limited to communications, messages, chats, emails, attachments, images, videos, electronic storage, “follower” and/or “friend” lists, subscriber information, terms of service violation reports, detailed billing records, which appears to contain passwords or information regarding encryption;
- d. Any and all transactional information, to include log files (transmission and usage) of all activity of the accounts, to include dates, times, methods of connecting, ports, dial-ups, locations, originating Internet Protocol (IP) addresses and/or destination IP addresses for any and all correspondence and/or content, to include but not limited to communications, messages, chats, emails, attachments, images, videos, electronic storage, “follower” and/or “friend” lists, subscriber information, terms of service violation reports, detailed billing records;
- e. All GPS or location information stored by Google, Inc. in relation to these accounts;
- f. Any records of subscriber information, methods of payment, or detailed billing; and,

g. Copies of all the above from original storage on whatever form, to include printouts
and/or digital format.